



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/404,547	09/24/1999	TAKESHI SAITO	0039-7378-2R	8485
22850	7590	04/07/2003		
OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C. FOURTH FLOOR 1755 JEFFERSON DAVIS HIGHWAY ARLINGTON, VA 22202			EXAMINER	
			TODD, GREGORY G	
			ART UNIT	PAPER NUMBER
			2157	10
DATE MAILED: 04/07/2003				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/404,547	SAITO ET AL.
	Examiner	Art Unit
	Gregory G Todd	2157

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
 If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
 Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 31 January 2003.
 2a) This action is **FINAL**. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-19 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-19 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 11) The proposed drawing correction filed on _____ is: a) approved b) disapproved by the Examiner.
 If approved, corrected drawings are required in reply to this Office action.
 12) The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
 * See the attached detailed Office action for a list of the certified copies not received.

14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
 a) The translation of the foreign language provisional application has been received.

15) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) <u>4.5</u> .	6) <input type="checkbox"/> Other: _____

DETAILED ACTION

Response to Amendment

1. This is a second office action in response to applicant's amendment filed, 04 February 2003, of application filed, with the above serial number, on 24 September 1999 in which claims 2, 6, 17, and 19 have been amended and claims 1, 3-5, 7-16, and 18 have been unaltered. Claims 1-19 are therefore pending in the application.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claims 1, 5-11, 14-16, and 19 are rejected under 35 U.S.C. 102(b) as being anticipated by Adams, Jr. et al (hereinafter "Adams", USPN 5,640,456).
2. As per claim 1, Adams discloses a relay device wherein Adams discloses:
 - a first interface unit (port) connected to a first network (see Fig. 2, ref. 12; col. 4 line 66 - col. 5 line 1);
 - a second interface unit (port) connected to a second network (see Fig. 2, ref. 14; col. 4 line 66 - col. 5 line 1);
 - a proxy configuration unit for disclosing a device/service/sub-unit on the second network as an own (transparent; It is interpreted by the office that disclosing a device/service/sub-unit on a network as an own device/service/sub-unit, as acting

transparent to a different network) device/service/sub-unit provided on the relay device with respect to a first network side (at least col. 4, lines 37-39);

- a control command reception unit (control terminal) for receiving control command signals destined to the own device/service/sub-unit from the first network side (at least col. 1, lines 47-58; col. 5, lines 12-20);

- a control command transmission unit (control terminal) for transmitting signals corresponding to the control command signals received by the control command reception unit, to the device/service/sub-unit on the second network (at least col. 1, lines 47-58; col. 5, lines 12-20);

- a contents protection information reception unit (part of the downstream port; at least col. 5, lines 2-5; col. 5 line 61 - col. 6 line 5) for receiving contents protection information (header characters with encryption/decryption information) destined to the own device/service/sub-unit, from a device on the first network (at least col. 6, lines 21-29; col. 4, lines 40-52);

- a contents protection information transfer unit (part of the upstream port; at least col. 5, lines 2-5; col. 5 line 61 - col. 6 line 5) for transferring the contents protection information (header characters with encryption/decryption information) received by the contents protection information reception unit to the device/service/sub-unit on the second network, without making any change (passed through without modification) in the contents protection information (at least col. 6, lines 21-29; col. 4, lines 40-52).

3. As per claim 5, Adams discloses a relay device wherein Adams discloses:

- a first interface unit connected to a first network (see Fig. 2, ref. 12; col. 4 line 66 - col. 5 line 1);
- a second interface unit connected to a second network (wherein 1394 bus is referred to as another network) (see Fig. 2, ref. 14; col. 4 line 66 - col. 5 line 1);
- a proxy configuration unit for disclosing each device/service/sub-unit on the first network or the second network as an own (transparent) device/service/sub-unit provided on the relay device with respect to respective another network side (at least col. 4, lines 37-39);
- a control command reception unit (control terminal) for receiving control command signals destined to the own device/service/sub-unit from a side of one network to which the own device/service/sub-unit is disclosed by the proxy configuration unit (at least col. 1, lines 47-58; col. 5, lines 12-20);
- a control command transmission unit (control terminal) for transmitting signals corresponding to the control command signals received by the control command reception unit, to said each device/service/sub-unit on another network different from said one network (at least col. 1, lines 47-58; col. 5, lines 12-20);
- a first contents protection unit for carrying out a contents protection procedure with respect to one device/service/sub-unit on the first network (downstream network port) (at least col. 6, lines 6-16, 21-29);
- a second contents protection unit for carrying out the contents protection procedure with respect to another device/service/sub-unit on the second network (upstream network port) (at least col. 6, lines 21-29; col. 6 line 65 - col. 7 line 11);

- a contents reception unit for receiving contents (data) destined to the own device/service/sub-unit and encrypted according to one of the first and second contents protection units (at least col. 6, lines 6-16, 21-29);

- a contents transfer unit for transferring the contents (data) received by the contents reception unit to said each device/service/sub-unit on said another network, by encrypting the contents according to another one of the first and second contents protection units (at least col. 6, lines 21-29; col. 6 line 65 - col. 7 line 11).

4. As per claim 6, Adams discloses a relay device wherein Adams discloses:

- the first contents protection unit and the second contents protection unit use identical encryption schemes based on different keys (the same encryption hardware is used with a key list for different keys and headers) (at least col. 4, lines 40-52).

5. As per claim 7, Adams discloses a relay device wherein Adams discloses:

- a contents reception unit and contents transmission unit (communications ports) sealed within a single LSI (microprocessor) (at least col. 5, lines 21-27).

6. As per claim 8, Adams discloses a relay device wherein Adams discloses:

- a first key information used in the contents protection procedure in the first contents protection unit and a second key information used in the contents protection procedure in the second contents protection unit are set to be identical (transferred header containing encryption information) (at least col. 6 line 65 - col. 7 line 11; col. 5 line 65 - col. 6 line 5).

7. As per claim 9, Adams discloses a relay device wherein Adams discloses:

- the contents protection procedure (encryption) in said another one of the first and second contents protection units carried out in units of contents/services/sub-units (packets), using a prescribed key information (header) (at least col. 5 line 61 - col. 6 line 11).

8. As per claim 10, Adams discloses a relay device wherein Adams discloses:

- a configuration information reception unit for receiving a configuration information (header) from one device/service/sub-unit on the first network or the second network, the configuration information indicating at least a presence or absence of an authentication format (indicate that data characters are encrypted) for said one device/service/sub-unit (at least col. 6, lines 3-5, 11-16, 25-29);

- a configuration recognition unit for recognizing (matching criteria) a configuration of said one device/service/sub-unit according to the configuration information received by the configuration information reception unit (at least col. 6, lines 3-5, 11-16, 25-29).

9. As per claim 11, Adams discloses a relay device wherein Adams discloses:

- a first interface unit connected to a first network (see Fig. 2, ref. 12; col. 4 line 66 - col. 5 line 1);

- a second interface unit connected to a second network (wherein 1394 bus is referred to as another network) (see Fig. 2, ref. 14; col. 4 line 66 - col. 5 line 1);

- a first contents protection unit for carrying out a contents protection procedure with respect to one device/service/sub-unit on the first network (downstream network port) (at least col. 6, lines 6-16, 21-29);

- a second contents protection unit for carrying out the contents protection procedure with respect to another device/service/sub-unit on the second network (upstream network port) (at least col. 6, lines 21-29; col. 6 line 65 - col. 7 line 11);
- a contents reception unit for receiving contents (data) destined to an own device/service/sub-unit on the relay device and encrypted according to one of the first and second contents protection units, from a device on one of the first network and the second network (at least col. 6, lines 6-16, 21-29);
- a contents transmission unit for transmitting the contents (data) received by the contents reception unit to a device/service/sub-unit on another one of the first network and the second network, by encrypting the contents according to another one of the first and second contents protection units (at least col. 6, lines 21-29; col. 6 line 65 - col. 7 line 11);
- wherein a first key information used in the contents protection procedure in the first contents protection unit and a second key information used in the contents protection procedure in the second contents protection unit are set to be identical (transferred header containing identical encryption information) (at least col. 6 line 65 - col. 7 line 11; col. 5 line 65 - col. 6 line 5).

10. As per claim 14, Adams discloses a communication device wherein Adams discloses:

- an interface unit connected to a network (see Fig. 2; col. 4 line 66 - col. 5 line 1);

- a contents transfer unit for transmitting or receiving encrypted contents with respect to another device on the network, through a flow identified by a set of a source address, a source port, a destination address, and a destination port (at least col. 4, lines 40-44; col. 5 line 65 - col. 6 line 5; col. 6, lines 17-20);

- a copy protection processing unit for carrying out a prescribed contents protection procedure (encryption) including at least an authentication procedure and/or a key exchange procedure (plurality of keys for handling the packet) with respect to said another device, using a prescribed logical port, in units of the flow (encrypt data using a key from a key list)(at least col. 4, lines 40-52; col. 6, lines 21-29).

11. As per claim 15, Adams discloses a communication device wherein Adams discloses:

- an identifier of the flow is attached (in header) to information (data) exchanged in at least a part of procedures included in the prescribed contents protection procedure (at least col. 6 line 65 - col. 7 line 2).

12. As per claim 16, Adams discloses a communication device wherein Adams discloses:

- an interface unit connected to a network (see Fig. 2; col. 4 line 66 - col. 5 line 1);

- a copy protection processing unit for carrying out a prescribed contents protection procedure (encryption) including at least an authentication procedure and/or a key exchange procedure, with respect to another device on the network (at least col. 4, lines 40-52);

- a contents transmission and reception unit for transmitting or receiving encrypted contents to which an address of a transmitting side device is attached, either through a virtual channel on the network or in a form having an identifier by which the encrypted contents can be uniquely identified by said, transmitting side device further attached thereto, with respect to said another device (at least col. 6, lines 6-29; col. 6 line 65 - col. 7 line 11);

- wherein at least one of an identifier of a service, a sub-unit, a virtual channel, or a plug (various network layers) that carries out exchange of the encrypted contents, and an identifier (header) by which the encrypted contents can be uniquely identified by said transmitting side device, is attached to information (data) exchanged in at least a part of procedures included in the prescribed contents protection procedure (encryption) (at least col. 5 line 61 - col. 6 line 5).

13. As per claim 19, Adams discloses a relay device wherein Adams discloses:

- a first interface unit connected to a first network (see Fig. 2, ref. 12; col. 4 line 66 - col. 5 line 1);

- a second interface unit connected to a second network (see Fig. 2, ref. 14; col. 4 line 66 - col. 5 line 1);

- a first contents protection unit for carrying out a contents protection procedure with respect to one device/service/sub-unit on the first network (downstream network port) (at least col. 6, lines 6-16, 21-29);

- a second contents protection unit for carrying out the contents protection procedure with respect to another device/service/sub-unit on the second network (upstream network port) (at least col. 6, lines 21-29; col. 6 line 65 - col. 7 line 11);
- a contents reception unit for receiving contents (data) destined to an own device/service/sub-unit on the relay device and encrypted according to one of the first and second contents protection units, from a device on one of the first network and the second networks (at least col. 6, lines 6-16, 21-29);
- a contents transmission unit for transmitting the contents (data) received by the contents reception unit to a device/service/sub-unit on another one of the first network and the second network, by encrypting the contents according to another one of the first and second contents protection units (at least col. 6, lines 21-29; col. 6 line 65 - col. 7 line 11);
- wherein said one of the first and second contents protection units carries out an authentication and/or a key exchange with a device/service/sub-unit on said one of the first network and the second network by referring to a states of the contents reception unit and the contents transmission unit (bits in header), when there is a request for a procedure of the authentication and/or the key exchange with respect to said another one of the first and second contents protection units (at least col. 5 line 61 - col. 6 line 11).

Art Unit: 2157

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claims 2-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Adams, Jr. et al (hereinafter "Adams", USPN 5,640,456).

16. As per claim 2, Adams discloses a relay device wherein Adams discloses:

- a first interface unit; connected to a first network (see Fig. 2, ref. 12; col. 4 line 66 - col. 5 line 1);

- a second interface unit connected to a second network (see Fig. 2, ref. 14; col. 4 line 66 - col. 5 line 1);

- a proxy configuration unit for disclosing each device/service/sub-unit on the first network or the second network as an own (transparent) device/service/sub-unit provided on the relay device with respect to respective another network (at least col. 4, lines 37-39);

- a control command reception unit (control terminal) for receiving control command signals destined to the own device/service/sub-unit from a side of one network to which the own device/service/sub-unit is disclosed by the proxy configuration unit (at least col. 1, lines 47-58; col. 5, lines 12-20);

- a control command transmission unit (control terminal) for transmitting signals corresponding to the control command signals received by the control command

reception unit, to each device/service/sub-unit on another network different from said one network (at least col. 1, lines 47-58; col. 5, lines 12-20);

- a contents protection information reception unit (part of the upstream port; at least col. 5, lines 2-5; col. 5 line 61 - col. 6 line 5) for receiving contents protection information destined to the own device/service/sub-unit: from a device on the first network or the second network (at least col. 6, lines 21-29; col. 4, lines 40-52);

- a contents protection information transfer unit (part of the upstream port; at least col. 5, lines 2-5; col. 5 line 61 - col. 6 line 5) for transferring the contents protection information received by the contents protection information reception unit to said each device/service/sub-unit on said another network, without making any change (passed through without modification) in the contents protection information (at least col. 6, lines 21-29; col. 4, lines 40-52);

Adams discloses encrypting data before it is sent over the network, thereby keeping a header and trailer intact and not encrypted (at least col. 2, lines 37-40). Adams also discloses passing through packets (containing a header, trailer, and data) without making any change (at least col. 4, lines 43-46). Adams' device also has decrypting hardware which suggests the data coming from the first network is encrypted, and he discloses the data being passed through without modification. Further, Adams discloses part of the header of the packet (contents) indicating the data as being encrypted (at least col. 6, lines 3-5) which suggests the reception unit receiving an encrypted packet. Adams does not explicitly disclose **a contents reception unit for receiving contents (data portion) destined to the own device/service/sub-unit and**

protected by a contents key obtained from the contents protection information, from a device on the first network or the second network (see col. 4, lines 30-32, 40-46; col. 2, lines 25-40), or a contents transfer unit for transferring the contents (data portion) received by the contents reception unit to said each device/service/sub-unit on said another network, without making any change (passed through) in the contents (see col. 4, lines 30-32, 40-46; col. 2, lines 25-40).

However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to also have encrypted data passed through the network because, as Adams teaches in the background art, older or incompatible systems could have encrypted the data before being sent over the network (see col. 2, lines 37-40), and therefore this would make the device compatible with these older systems.

17. As per claim 3, Adams discloses a relay device wherein Adams discloses:

- contents protection information (header) related to a contents protection procedure including an authentication and/or a key exchange between one device/service/sub-unit on the first network and another device/service/sub-unit on the second network (information of the data encrypted on one network and decrypted on the other network is contained in header) (at least col. 5 line 65 - col. 6 line 5).

18. As per claim 4, Adams discloses a relay device wherein Adams discloses:

- a configuration information reception unit for receiving configuration information (option bit) from one device/service/sub-unit on the first network or the second network, the configuration information indicating at least a presence or absence of an

Art Unit: 2157

authentication format (indicate that data characters are encrypted) for said one device/service/sub-unit (at least col. 6, lines 3-5, 25-29);

- a configuration recognition unit for recognizing (compares) a configuration (information extracted from header according to key list) of said one device/service/sub-unit according to the configuration information (option bit in header) received by the configuration information reception unit (at least col. 6, lines 3-5, 11-16, 25-29).

19. Claims 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Adams, Jr. et al (hereinafter "Adams", USPN 5,640,456) in view of Perlman (hereinafter "Perlman", USPN 5,175,765).

20. As per claim 12, Adams discloses a communication device wherein Adams discloses:

- an interface unit connected to a network (see Fig. 2; col. 4 line 66 - col. 5 line 1);

- a copy protection processing unit for carrying out a prescribed contents protection procedure including at least an authentication procedure and/or a key exchange procedure (mechanism to maintain list of keys for sites so as to change key for respective site), with respect to another device/service/sub-unit on the network (at least col. 4, lines 40-52);

- a contents transmission unit for transmitting encrypted contents to which an address of the communication device is attached, either through a virtual channel on the network or by further attaching an identifier by which the encrypted contents can be

uniquely identified by the communication device, to another device on the network (at least col. 6, lines 21-29, 17-20; col. 6 line 65 - col. 7 line 11);

Adams fails to disclose a reception unit for receiving a query regarding a service/sub-unit/plug that is transferring the encrypted contents either through the virtual channel or by attaching the identifier, from said another device on the network, or a notification unit for notifying (transmitting to) a service/sub-unit/plug that is transferring the encrypted contents, to said another device on the network in response to the query. However, the use and advantages for querying over a network is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Perlman (at least col. 14, lines 38-49). Perlman discloses querying nodes from a site on the network and further, the nodes responding back from the query. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the ability to query into the device from Adams because this would ensure and detect that no packets (contents) are being lost in the communication path and that there is a stable, fault-free connection between the device and a node on one of the networks, especially when first setting up the device between the two networks.

21. As per claim 13, Adams discloses a communication device wherein Adams discloses:

- an interface unit connected to a network (see Fig. 2; col. 4 line 66 - col. 5 line 1);

- a copy protection processing unit for carrying out a prescribed contents protection procedure (encryption) including at least an authentication procedure and/or a key exchange procedure, with respect to another device/service/sub-unit on the network (at least col. 4, lines 40-52);

- a contents reception unit for receiving encrypted contents to which an address of another device on the network is attached, either through a virtual channel on the network or in a form having an identifier by which the encrypted contents can be uniquely identified by said another device further attached thereto, from said another device (at least col. 6, lines 6-29);

Adams fails to disclose a transmission unit for transmitting a query regarding a service/sub-unit/plug that is transferring the encrypted contents either through the virtual channel or by attaching the identifier, to said another device on the network, or a reception unit for receiving a notification regarding a service/sub-unit/plug that is transferring the encrypted contents, from said another device in response to the query. However, the use and advantages for querying over a network is well known to one skilled in the art at the time the invention was made as evidenced by the teachings of Perlman (at least col. 14, lines 38-49). Perlman discloses querying nodes from a site on the network and further, the nodes responding back from the query. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the ability to query into the device from Adams because this would ensure and detect that no packets (contents) are being lost in the communication path and that there is a stable,

fault-free connection between the device and a node on one of the networks, especially when first setting up the device between the two networks.

22. Claims 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Adams, Jr. et al (hereinafter "Adams", USPN 5,640,456) in view of Saito (hereinafter "Saito", EP 0 837 579).

23. As per claim 17, Adams discloses a relay device wherein Adams discloses:

- a first interface unit; connected to a first network (see Fig. 2, ref. 12; col. 4 line 66 - col. 5 line 1);
 - a second interface unit connected to a second network (wherein 1394 bus is referred to as another network) (see Fig. 2, ref. 14; col. 4 line 66 - col. 5 line 1);
 - a first copy protection processing unit for carrying out a prescribed contents protection procedure including at least an authentication procedure and a key exchange procedure (mechanism to maintain list of keys for sites so as to change key for respective site), with respect to one device/service/sub-unit on the first network (at least col. 4, lines 40-52);
 - a second copy protection processing unit for carrying out the prescribed contents protection procedure including at least an authentication procedure and a key exchange procedure (mechanism to maintain list of keys for sites so as to change key for respective site), with respect to another device/service/sub-unit on the second network (at least col. 4, lines 40-52);
 - a contents reception unit for receiving encrypted data containing contents from the first interface unit (at least col. 6, lines 6-16, 21-29);

- a decryption unit for decrypting the encrypted data received by the contents reception unit, by using a contents protection key provided by the first copy protection processing unit, to obtain decrypted data (at least col. 7, lines 19-33);
- an encryption unit for encrypting the converted data (see below), by using a contents protection key (compare header information with key list) provided by the second copy protection processing unit, to obtain re-encrypted data (at least col. 6, lines 6-16);
- a contents transmission unit for transferring the re-encrypted data to the second interface unit (at least col. 6 line 65 - col. 7 line 11).

Adams fails to disclose **a conversion unit for converting the decrypted data into converted data in another coding format**. However, the use and advantages for converting such data is well known to one skilled in the relevant art at the time the invention was made as evidenced by the teachings of Saito (at least col. 29, lines 17-30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate a conversion unit in Adams' device because this would be more efficient, and sometimes necessary depending on the particular device, for the receiving device to automatically have the data converted to the correct and readable format for that particular network device, while at the same time the data being securely transmitted by being encrypted with Adams device.

24. As per claim 18, Adams discloses a relay device wherein Adams discloses:

- a proxy configuration unit for disclosing one device/service/sub-unit on the second network as one own (transparent) device/service/sub-unit provided on the relay

device with respect to a first network side (at least col. 4, lines 37-39), and transmitting to said one device/service/sub-unit on the second network an information having a content (data) according to information (header) destined to said one own device/service/sub-unit that is received from a device on the first network side (transmit packet from first network to second network (downstream)) (see Fig. 7; at least col. 7, lines 51-54), while also disclosing another device/service/sub-unit on the first network as another own device/service/sub-unit provided on the relay device with respect to a second network side (the device is transparent to both sides; It is implied that disclosing a device/service/sub-unit on a network as an own device/service/sub-unit is equivalent to acting transparent to a different network) (at least col. 4, lines 26-39), and transmitting to said another device/service/sub-unit on the first network an information (header) having a content (data) according to information destined to said another own device/service/sub-unit that is received from a device on the second network side (transmit packet from second network to first network (upstream)) (see Fig. 7; at least col. 7, lines 8-12);

- when the prescribed contents protection procedure between a device on one network among the first and second networks and a device/service/sub-unit on another network among the first and second networks is to be carried out, the proxy configuration unit carries out the prescribed contents protection procedure with the device on said one network by using one of the first and second copy protection processing units, while carrying out the prescribed contents protection procedure with the device/service/sub-unit on said another network by using another one of the first

and second copy protection processing units (the contents protection procedure (encryption) is carried out between a device (computer) on first network and another device (computer) on another network) (at least col. 4, lines 37-59).

Response to Arguments

25. Applicant's arguments filed 30 January 2003 have been fully considered but they are not persuasive. The applicant argues in substance that: a) Adams is silent of a proxy unit to ensure the device on a second network is viewed as being on the first network (transparent) with respect to claim 1; b) Adams does not disclose the use of control command reception and transmission units for controlling signals from one network to another and that Adams only suggests transferring control signals inside the relay device itself; c) Adams does not disclose a contents protection information reception and transfer unit; d) Adams does not disclose first and second content protection units for a device on a first and second network, respectively; e) Adams does not disclose first and second key information as being identical; f) Adams does not disclose the contents transfer unit tx/rx through the flow (source/dest port and addresses); g) Adams does not disclose using a contents protection unit (copy protection unit) according to a key exchange procedure; h) Adams does not disclose an identifier to identify encrypted contents and an identifier of the service; i) Adams does not disclose transferring contents transparently; j) Perlman's query and response is not a query and encrypted contents.

In response to a); The claim 1 terminology suggests that in order for the device on the second network to act as an own device on the first network, the device on the second network being provided on and connected to the relay device, it will be transparent and therefore the relay device acting transparent from both networks.

In response to b); Adams clearly discloses the control terminal (reception and transmission) as controlling the keylist (at least col. 5, lines 12-20). This controlling of the keylist is done by header information, being packeted from a network node, having information as to what the keylist should do with the packet, thus how to control it (at least col. 6, lines 6-29).

In response to c); Adams clearly discloses, as the applicant agrees, the relay device as being able to act transparently as previously cited (at least col. 6, lines 21-29). Adams discloses the packet header having control information to control the relay device to have the data (encrypted, unencrypted, etc.; the relay device is unaware as to the status of the data, as it is not necessary) passed through without any modification and thus transparently. Adams discloses the control signals being packed into the packet header at one network side to act along with the contents protection information on allowing the relay device to act transparently and not make any change to the contents protection information.

In response to d); Adams discloses his relay device's contents protection unit acting according to packet header information parsed from a packet from the upstream or downstream ports (at least Fig. 6; col. 6, lines 6-21) acting transparently to the other

network side and thus each port acting as having a separate 'unit' to provide contents protection.

In response to e); Adams discloses the key as being stored and used according to the destination (at least col. 6, lines 59-64, 17-20), and then further encrypted/decrypted (contents protection procedure) according to this key, the key being selected according to the destination/source addresses, and thus this same key must be used and identical for the two addresses to communicate properly and the data be extracted accordingly.

In response to f); Adams clearly discloses transferring contents according to header information (this information containing source/dest port/address) (at least col. 6, lines 6-20) and using masking to determine which sub-network/network. It was well known in the art at the time the invention was made that a packet header contains a source/dest port/addresses as Adams discloses (at least col. 5, lines 65-67) and thus Adams clearly transfers data according to the header information.

In response to g); Adams clearly discloses using an authentication / key exchange procedure through the use of a key list and encryption process (at least col. 5 line 61 - col. 6 line 5; col. 6, lines 21-29). Data is clearly authenticated when it is associated and decrypted using a key. Further, when the option bit Adams discloses indicates the data is secure, it must be authenticated with a key either through the relay device itself or at the source/dest address.

In response to h); Adams discloses the relay device inserting header and trailer characters in the packet to indicate the data had been encrypted, for instance, via the

option bit, and thus if the data has been encrypted, it has been indicated in the header to be encrypted, the relay device connecting the two networks, thus the destination address receiving encrypted contents indicating the relay device having done the encryption (at least col. 5 line 61 - col. 6 line 5).

In response to i); See remarks for argument a) with respect to similar claim 1.

In response to j); Perlman discloses querying for packet reception and responding with a confirmation (at least col. 14, lines 38-49). This reads on the claim of the reception unit receiving a query from another device on the network and notification unit for responding to the query. The claim language does not suggest receiving encrypted contents and only for updating packet reception status.

Conclusion

26. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Art Unit: 2157

27. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Lea, Vu, Daniels et al, Templin et al, Kimura et al, Sharpe, and Brewer are cited for disclosing pertinent information related to the claimed invention. Applicants are requested to consider the prior art reference for relevant teachings when responding to this office action.

28. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gregory G Todd whose telephone number is (703)305-5343. The examiner can normally be reached on Monday - Friday 9:00am-6:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (703)308-7562. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)305-3900.

gt
April 1, 2003



SALEH NAJJAR
PRIMARY EXAMINER